




## Procedures and Guidelines (PG)

**DIRECTIVE NO.** 800-PG-7150.4.1  
**EFFECTIVE DATE:** July 15, 2013  
**EXPIRATION DATE:** July 15, 2020

**APPROVED BY Signature:**   
**NAME:** David L. Pierce  
**TITLE:** Director, Wallops Flight Facility

---

### COMPLIANCE IS MANDATORY

---

**Responsible Office:** 803/Safety Office

**Title:** Software Safety and Mission Assurance Process Interface

---

## PREFACE

### P.1 PURPOSE

This procedure documents the interface between the Goddard Space Flight Center/Wallops Flight Facility (GSFC/WFF) Safety Office (Code 803) and WFF Programs/Projects for facility-level software safety and mission assurance activities.

### P.2 APPLICABILITY

This procedure applies to software assurance for engineering activities performed by or for Code 800 Programs/Projects and their support civil servants and contractors.

This directive is not mandatory for software development, maintenance, operations, management, acquisition, and assurance activities started before September 27, 2004 (the initial issuance of NPR 7150.2A NASA Software Engineering Requirements).

In this document, requirements apply to acquirer software activities and in-house provider software activities. When requirements apply to external software activities (acquisitions), "external" is specified.

### P.3 AUTHORITY

NPR 7150.2, NASA Software Engineering Requirements

### P.4 REFERENCES

NPR 1441.1, NASA Records Retention Schedules

NPR 7150.2, NASA Software Engineering Requirements

NASA-STD-8709.20, Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements

NASA-STD-8709.22, Safety and Mission Assurance Acronyms, Abbreviations, and Definitions.

NASA-STD-8719.13, Software Safety Standard

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** 800-PG-7150.4.1  
**EFFECTIVE DATE:** July 15, 2013  
**EXPIRATION DATE:** July 15, 2020

Page 2 of 17

NASA-STD-8739.8, Software Assurance Standard  
GPR 5340.2, Control of Process Nonconformances and Customer Complaints  
GPR 7150.4, Software Safety and Software Reliability Process  
803-PG-8715.1.2, Range Safety Deviation and Waiver Process  
RSM 2002, Range Safety Manual for Goddard Space Flight Center/Wallops Flight Facility

## P.5 CANCELLATION

This directive combined with the Code 803 Software Safety and Mission Assurance Process directive replaces 589-SW-ASSURANCE-PLAN-01, Wallops Flight Facility Software Quality Assurance (SQA) Plan (Revision 2, April 2011).

## P.6 SAFETY

N/A

## P.7 TRAINING

N/A

## P.8 RECORDS

Record Title	Record Custodian	*Retention (at a minimum)
Software Assurance Classification Reports and Software Safety Criticality Assessments (official records and/or references)	WFF Safety Office, Software Assurance Manager	<u>NRRS 8/107</u> Temporary, Destroy/delete when no longer needed. <i>(Until the end of the software system's lifecycle when the information becomes obsolete)</i>
Software Inventory Software Assurance Information (planned and actual effort per software project)	"	<u>NRRS 1/26.5A</u> For quality management files recordkeeping - destroy when 7 years old. or <u>NRRS 1/26.5C</u> until updates are entered into a NASA Software Inventory Management System (SIMS) making local copies obsolete
Software Safety Reports (planned and actual assessments, open and closed software project concerns and risks)	"	<u>NRRS 1/26.5A</u>

\*NRRS - NASA Records Retention Schedules (NPR 1441.1)

Records are maintained in accordance with the Safety Office Organization File Plan.

## P.9 MEASUREMENT/VERIFICATION

The WFF Safety Office will provide periodic (at a minimum semiannual) Software Safety Reports to Programs/Projects and/or the Product Development Lead (PDL) for each project requiring software

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

assurance and safety activities. Reports will summarize (a) planned and actual Safety Office product and process assessments and (b) open and closed concerns and risks.

If an assessment indicates a NASA Software Safety Standard (NASA-STD-8719.13) or NASA Software Assurance Standard (NASA-STD-8739.8) requirement will not be met, the Program/Project will follow the Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements (NASA-STD-8709.20) process to obtain approval for a variance.

## PROCEDURES

In this document, a requirement is identified by “shall,” a good practice by “should,” permission by “may” or “can,” expectation by “will,” and descriptive material by “is.”

In this document, Software Safety and Mission Assurance Process Interface requirements are identified as “SSMAPI-” followed by a unique number.

In this document, a WFF Program/“Project” is an item from the Master Agency Project List, typically identified by the first 6 digits of a Work Breakdown Structure charge number. A software “project” is an effort associated with a specific software system or software inventory item. The term “project,” used without qualification, refers to a software project.

The Safety Office defines three types of software assurance and safety activities in this directive: Monitoring, Insight, and Oversight. The applicability of each activity type to a software project is based on the software’s classification and safety-criticality. Software classes are defined in NPR 7150.2, NASA Software Engineering Requirements.

- **Monitoring activities** (e.g., software classification and criticality assessment) apply to all Class A-E software systems.
- **Insight activities** (e.g., periodic process audits) apply to all Class A-C and only safety-critical Class D-E software systems.
- **Oversight activities** (e.g., involvement in safety requirements definition, hazard analysis, and critical tests) apply to all Class A-B and only safety-critical Class C-E software systems. However, Projects may also request oversight for non-safety-critical Class C-E software systems.

## 1.0 ROLES

This Software Safety and Mission Assurance Process Interface procedure and the Safety Office’s Software Safety and Mission Assurance Process work instruction, together, define how the WFF Suborbital and Special Orbital Projects Directorate (Code 800) implements the requirements of the NASA Software Assurance Standard, the NASA Software Safety Standard, and the GSFC Software Safety and Software Reliability Process for WFF software system acquisition, development, maintenance, retirement, operations, and management. Applicable requirements are defined by role.

<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

- 1.1 The Safety Office assumes the role of the software acquirer Safety and Mission Assurance (SMA) organization. For WFF in-house software development, maintenance, retirement, operations, and management efforts, the Safety Office also assumes the role of the software provider SMA organization.
- 1.2 Programs/Projects assume the role of acquirer management and for in-house efforts the role of provider management. Providers are typically software project teams.

## 2.0 RESPONSIBILITIES

- 2.1 The Safety Office is responsible for defining, leading, and staffing the facility-level software assurance and safety activities.
  - 2.1.1 The Safety Office's Range Safety Officer will certify safety-critical software systems for operational use.
  - 2.1.2 The Safety Office Chief shall identify a Safety Office Software Assurance Manager to maintain and lead the implementation of the Software Safety and Mission Assurance Plan [SSMAPI-001].
  - 2.1.3 The Safety Office Chief will ensure trained engineers and/or specialists are assigned to support software safety and assurance activities. The Safety Office will provide Safety Office points of contact for software projects.
  - 2.1.4 The Safety Office may schedule facility software assurance and software safety training.
  - 2.1.5 The Safety Office will provide process and product assessments, as defined in Section 3.0. The Safety Office may request or consent to the transfer of some or all of Section 3.0 Safety Office responsibilities to another SMA organization. A transfer of acquirer SMA responsibilities or in-house provider SMA responsibilities must be documented in an assurance and safety plan supplement approved by the Safety Office and affected Program/Project organizations.
- 2.2 Programs/Projects are responsible for providing information and funding to enable the activities.
  - 2.2.1 Programs/Projects shall work with the Safety Office Chief to establish adequate resources for each Safety Office software assurance and software safety activity [SSMAPI-002].
    - 2.2.1.1 Resources for monitoring and insight activities affecting multiple projects will be determined annually. Resources for project-specific oversight activities will be determined at the start of each project and re-evaluated at least annually. Resource estimates for similar projects may be grouped to allow software assurance and safety support to move with software engineering priorities.
    - 2.2.1.2 Each Program/Project will provide funding for Safety Office software safety and software assurance support and associated training and management costs.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



2.2.1.3 Each Program/Project will implement a process or mechanism to respond to reported nonconformances, concerns, and risks.

2.2.2 Programs/Projects will provide process and product information, as defined in Section 3.0.

2.3 In the event of a funding or staffing shortage, the Safety Office will work with the Programs/Projects to prioritize planned work.

### 3.0 INFORMATION EXCHANGE

The type of information to be exchanged depends on software classification and safety-criticality. Software classifications are defined in NPR 7150.2, NASA Software Engineering Requirements.

3.1 Monitoring for Class A-E software systems (NPR 7150.2 classes)

The Safety Office will continually monitor WFF software activities to identify critical software system changes, including procurement or development of new systems, updates to existing systems, changes to how systems are used, and observed system faults or failures. Monitoring also provides an inventory of efforts for Class A to E software systems.

3.1.1 To enable monitoring activities, Programs/Projects will provide the following information:

Information Type	Applicability
a. <b>Project Initiation Reports</b> – Notification of the development/procurement of new software systems and information about new software systems, usually a software classification request during the Initiation or Pre-award lifecycle phase	for Class A-E software systems (mission, research, science, or engineering software created or acquired by or for Code 800, but not business or information technology infrastructure software)
b. <b>Project Software Class/Safety Updates</b> – Additions or changes to software system information, often affecting software classification or NASA software inventory reports	
c. <b>Control Board Change Requests</b> – Planned changes to operational systems, emphasizing affects on safety critical systems	for systems for which the Safety Office provides oversight (typically Class A-B software systems and Class C-E safety-critical software systems)
d. <b>New Operation Plan Reports</b> – Descriptions of how software systems will be used, emphasizing affects on safety critical systems	
e. <b>Software System Problem Reports</b> – Discrepancies reported for operational systems, emphasizing affects on safety critical systems	
f. <b>Software System Equivalent Oversight Evidence</b> – Information associated with a request for exemption from Safety Office oversight activities	an option for Class A-B software systems and Class C-E safety-critical software systems

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** 800-PG-7150.4.1  
**EFFECTIVE DATE:** July 15, 2013  
**EXPIRATION DATE:** July 15, 2020

Page 6 of 17

g.	<b>Software Project Oversight Requests</b> – Requests for Safety Office oversight (for systems/components for which the Safety Office would not typically provide oversight)	an option for Class C-E non-safety-critical software systems or for mission-critical components of Class A-B software systems
h.	<b>Software Contract Guidance Requests</b> – Notifications of contract planning and requests for software assurance and safety requirements, proposal evaluation, memorandum of understanding evaluation, memorandum of agreement evaluation, survey input, or assistance with contract negotiations	for contracts affecting any lifecycle phase for Class A-E software systems
i.	<b>Project Variance Requests</b> – Requests for a deviation or waiver for (request for relief from) a requirement. (See NASA-STD-8709.20 for requirements that trace to the NASA Software Safety Standard and NASA Software Assurance Standard. See the Range Safety Manual variance process for requirements that trace to NASA-NPR-8715.5 Range Safety Program.)	an option for Class A-E software systems (typically the safety-critical software systems)

3.1.1.1 Software Project Oversight Requests require the Safety Office Chief's approval. The Safety Office will maintain copies of approved Software Project oversight Requests.

3.1.1.2 Project Variance Requests for software assurance, software safety, or range safety requirements require Safety Office approval. The Safety Office will maintain copies of approved Project Variance Requests.

3.1.2 As a result of monitoring activities, the Safety Office will provide the following information:

Information Type		Applicability
a.	<b>Software Classification Forms</b> – Software classification assessments, software safety criticality assessments, and level of software assurance and software safety activities (e.g., whether or not Safety Office oversight is planned)	for Class A-E software systems
b.	<b>Software Inventory Updates</b> – Software project, assurance, and safety information provided for periodic NASA software inventory updates requested by the NASA Chief Engineer in coordination with NASA SMA organizations.	
c.	<b>Software Contract Guidance</b> – Software assurance and safety requirements, proposal evaluation, memorandum of understanding evaluation, memorandum of agreement evaluation, survey input, or assistance with contract negotiations	for contracts affecting any lifecycle phase for Class A-E software systems
d.	<b>System Hazard Analysis Updates</b> – Safety Office analysis used to identifies the high-level safety-critical aspects of software systems	for systems that contain safety-critical software

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



3.1.2.1 A Program/Project initiates the software classification and safety criticality assessment by providing project information. The Safety Office and the Program/Project work together to determine the software class and safety criticality. If necessary, disagreements may be resolved by elevating concerns through the NASA Technical Authority SMA chain (see NASA-STD-8709.20).

3.1.2.2 Projects may take responsibility for documenting software classification and safety-criticality (e.g., on the GSFC Project Initiation Form). If project-controlled classification and criticality information is approved by the Safety Office software assurance manager and approved by the Range Safety Officer for safety-critical software systems, then the Safety Office will keep a copy of the approved form with a link to the official controlled record.

3.1.3 Programs/Projects and the Safety Office shall implement the following monitoring artifact constraints [SSMAPI-003]:

Subject		Agreement Constraint
a.	<b>Software Classification Forms</b>	Software Classification Forms are approved by both a Program/Project's software project representative and a Safety Office software assurance representative.  Software Classification Forms for safety-critical systems are approved by the Range Safety Officer.  Software Classification Forms are re-evaluated at a minimum at each project major milestone review.
b.	<b>Control Board Change Requests</b>	Change Requests for safety-critical systems require concurrence of the Range Safety Officer.
c.	<b>Software System Problem Reports</b>	Dispositions of Problem Reports for safety-critical systems require concurrence of the Range Safety Officer.
d.	<b>Project Variance Requests</b>	Variance Requests are evaluated by the Safety Office.  As one step in the approval process, the Range Safety Officer, as the Range Safety Technical Authority, approves variance requests for safety-critical requirements that trace to NASA-NPR-8715.5 Range Safety Program.

3.2 Insight for Class A-C and safety-critical Class D-E software systems (NPR-7150.2 classes)

The Safety Office performs insight audits to ensure (a) processes are documented and approved, (b) processes accomplish intended purposes, and (c) processes are followed. The Safety Office shall perform periodic software audits for Class A, B, and C software systems and for safety-critical Class D and E software systems [SSMAPI-004].

3.2.1 The number of audits and audit schedule will be determined annually.

- 3.2.1.1 The Safety Office will select a sampling of projects to audit each year. The list of selected projects will be given to Programs/Projects.
- 3.2.1.2 The Safety Office and Programs/Projects will determine the audit schedule.
- 3.2.1.3 The number of planned audits may be decreased in the event of a funding or staffing shortage.
- 3.2.2 The Safety Office may obtain assistance from civil servant or contracted auditing organizations, independent of Programs/Projects, (e.g., the GSFC Software Assurance Office in Greenbelt).
- 3.2.3 To enable audit activities, Programs/Projects will provide the following project process artifacts and evidence:

Software Artifact/Evidence		Description	Applicability
a.	<b>Configuration Management Plans</b>	Process definition documentation showing compliance with NASA process requirements and approval by appropriate authorities	for all Lifecycle Phases
b.	<b>Assurance Plans</b>		
c.	<b>Safety Plans</b>		for Safety-Critical Systems for all Lifecycle Phases
d.	<b>Management Plans/Product Plans</b> (including Risk Management)		for Development Phases
e.	<b>Test Plans and Procedures</b> (including initial development and regression testing)		for Test Phases
f.	<b>Maintenance and Operation Plans</b>		
g.	<b>User Manuals</b> (including identification/tagging of safety-critical components)		for Operational Systems
h.	<b>Retirement Plans</b>		
i.	<b>Controlled Items</b> (e.g., Code/Executables, Compliance Matrices) and <b>Records</b> (e.g., Assessment Results)	Evidence of following defined processes for the current project phase and evidence each process effectively meets its intended purpose	for Current Phase Processes
j.	<b>Interview Responses</b>		

- 3.2.3.1 In-house software projects should refer to this Software Safety and Mission Assurance Process Interface procedure and the Safety Office's Software Safety and Mission Assurance Process work instruction as the facility-level software assurance and safety plans.
- 3.2.3.2 Information should be provided in an electronic format if possible.
- 3.2.3.3 Projects/Programs will advise the Safety Office of any contract limitations or other restrictions preventing or delaying audits. The list of expected artifacts may be tailored for projects external to WFF (acquisitions).

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

3.2.4 As a result of audit activities, the Safety Office will provide the following information:

Information Type		Applicability
a.	<b>Concerns/Risk Reports</b> – Components of the Safety Office periodic (at a minimum semiannual) Software Safety Reports  A description of any tailoring of the list of expected audit artifacts will be noted.	for software assurance and safety concerns/risks
b.	<b>Nonconformance Reports</b> – Entries into the GSFC Audit/NCR System (see GPR 5340.2)	for nonconformances to current NASA and GSFC process requirements for which objective evidence has been collected

- 3.2.4.1 Project-specific concerns and risks are reported to each software project lead. If not resolved by the lead, the concerns and risks may be elevated to the Program/Project management or systems engineer.
- 3.2.4.2 Personnel names are not included in audit concerns/risk reports and nonconformance reports. To focus on organization process compliance instead of individual process compliance, audit results of similar small projects under the same Program/Project may be combined in concern/risk reports and noncompliance reports.
- 3.2.5 Programs/Projects and the Safety Office shall implement the following process document constraints [SSMAPI-005]:

Subject		Agreement Constraint
a.	<b>Safety Plans</b>	For safety-critical software projects external to WFF (acquisitions), the Safety Office approves the provider software safety plan. (The Safety Office provides the software safety plan for in-house safety-critical software projects.)
b.	<b>Test Plans and Procedures</b>	The Safety Office concurs on safety-related test plans and procedures.  The Safety Office concurs on plans to replace verification and validation by test with verification and validation by analysis, demonstration, or inspection, for software safety requirements that cannot be verified and validated by test.
c.	<b>Retirement Plans</b>	For safety-critical systems, the Safety Office concurs on how retirement/replacement plans address software safety.

### 3.3 Oversight for Class A-B and safety-critical Class C-E software systems (NPR 7150.2 classes)

The Safety Office shall provide oversight for Class A and B software projects and for safety-critical Class C, D, and E software projects [SSMAPI-006]. Programs/Projects may also request the Safety Office Chief's approval for Safety Office oversight of non-safety-critical Class C, D, and E projects.

3.3.1 For each project, the oversight process includes (1) determining required safety-critical function reliability level, (2) creating/updating software hazard analysis, and (3) assessing project artifacts for evidence of safe critical function. Safety Office oversight activities will be integrated with software project schedules.

3.3.2 To enable project oversight activities, Programs/Projects will provide the process artifacts and evidence listed for process audits (under 3.2.3) and the following project product artifacts and evidence:

Software Artifact/Evidence		Description	Applicability
a.	<b>Requirements Specifications</b> (including analysis and identification/tagging of safety-critical components)	Controlled or delivered items resulting from following project processes	by Preliminary Design Phase (initially)
b.	<b>Metric Reports</b>		(prior to releasing requirements for a contract)
c.	<b>Peer Review/Inspection Reports</b>		for Safety-Critical Systems by Detailed Design Phase
d.	<b>Hazard Analyses*</b> (including safety data and analysis)		
e.	<b>Data Dictionaries</b>		
f.	<b>Software Design Descriptions</b> (including identification/tagging of safety-critical components and trace to requirements)		by Detailed Design Phase
g.	<b>Interface Design Descriptions</b>		
h.	<b>Code and associated Files</b> (including identification/tagging of safety-critical components and trace to design)		by Implementation Phase
i.	<b>Version Descriptions</b>		
j.	<b>Change Requests/Problem Reports</b>		
k.	<b>Test Reports</b> (including data and analysis and including identification/tagging of safety-critical components and trace to requirements/design/code)		by Test Phase
l.	<b>Other Controlled Items and Records</b>	Quality, Safety, Reliability, and Verification & Validation Information	for Current Phase
m.	<b>Project Discussions</b> (e.g., Meeting, Reviews)		

\* Software safety engineers assist projects team with the creation of hazard analysis.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



3.3.2.1 Software project teams provide the Safety Office with product and process artifacts and all updates to the artifacts.

3.3.2.2 Information should be provided in an electronic format if possible.

3.3.2.3 Projects/Programs will advise the Safety Office of any contract limitations or other restrictions preventing or delaying oversight activities. The list of expected artifacts may be tailored for projects external to WFF (acquisitions).

3.3.3 As a result of project oversight activities, the Safety Office will provide the following information:

Information Type		Applicability
a.	<b>Inputs to Project Plans</b> (including software assurance and safety plans and safety-related test plans)	For planning phases
b.	<b>Hazard Analysis*</b> – Part of the system safety analysis; applies to new software, reused software, and off-the-shelf software	Updated throughout the project's lifecycle
c.	<b>Inputs to Formal Reviews</b> – The Safety Office reports on software system quality, significant concerns/risks, and compliance with the NASA software assurance and software safety directives.	For each formal or milestone review
d.	<b>Concerns/Risk Reports</b> – Components of the Safety Office periodic (at a minimum semiannual) Software Safety Reports.  A description of any tailoring of the list of expected audit artifacts will be noted.	For project-specific concerns/risks throughout the project's lifecycle
e.	<b>Nonconformance Reports</b> – Entries into the GSFC the Audit/NCR System (see GPR 5340.2)	For nonconformances to current NASA and GSFC process requirements for which objective evidence has been collected
f.	<b>Certification Memorandum</b>	For safety-critical software systems

\* *Software safety engineers assist projects team with the creation of hazard analysis.*

3.3.4 Programs/Projects and the Safety Office shall implement the constraints for process documents listed in section 3.2.5 and the following product oversight constraints [SSMAPI-007]:

**DIRECTIVE NO.** 800-PG-7150.4.1  
**EFFECTIVE DATE:** July 15, 2013  
**EXPIRATION DATE:** July 15, 2020

Page 12 of 17

Subject		Agreement Constraint
a.	<b>Software Safety Requirements</b>	The Safety Office approves the safety requirements.
		The Safety Office concurs on the unique identification/tagging of safety requirements.
b.	<b>Hazard Analysis</b>	The Safety Office concurs on the trace of safety requirements to software-related hazards, controls, conditions, and events and associated controls, mitigations, and inhibits.
		The Safety Office approves the software hazard analysis.  The Safety Office concurs on identification of software-related hazards, conditions, or events, along with the associated controls, mitigations, or inhibits.  (Updates are expected following analysis of design, implementation, and test.)
c.	<b>Test Reports</b>	The Safety Office concurs on safety-related software system verification and validation results.
d.	<b>Project Discussions</b>	A Safety Office representative is an approving member of the decision body at all major milestone and safety reviews.
e.	<b>Concerns/Risk Reports</b>	Project-specific concerns and risks are reported to each software project lead. If not resolved by the lead, the concerns and risks may be elevated to the Program/Project management or systems engineer.
f.	<b>Certification Memorandum</b>	The Safety Office certifies safety-critical software systems for operational use, based on project artifacts, evidence and acceptance documentation.

3.3.4.1 Software project teams will uniquely identify/tag safety-critical project elements, including requirements, design components, code, test plans, test procedures, and test results. The Safety Office will concur with the identification/tagging of safety-critical elements.

3.3.4.2 The Project/Program and the Safety Office will negotiate a schedule to allow the Safety Office to witness formal and acceptance-level software testing.

3.3.4.2.1 Testing verifies the correct and safe operation of the software in conjunction with system hardware and operator inputs in all anticipated nominal operational configurations and under load, stress, and other off-nominal configurations.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

Page 13 of 17

- 3.3.4.2.2 Testing includes the operation of software safety controls and mitigations, includes the ability to transition to a safe state. This includes testing in the presence of failures and faults including software, hardware, input, timing, memory corruption, communication, and other failures or conditions that impact safety-critical system performance, based on a hazard analysis. Testing verifies and validates that system hazards/fault-tree events/potential failure modes and risks related to software have been eliminated or controlled.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

## Appendix A – Definitions

Additional definitions for safety and mission assurance terms are found in NASA-STD-8709.22, Safety and Mission Assurance Acronyms, Abbreviations, and Definitions.

- A.1 Acquirer – The entity or individual who specifies the requirements and accepts the resulting software products. The acquirer is usually NASA or an organization within the Agency but can also refer to the Prime contractor – subcontractor relationship as well.
- A.2 Approve - For this document, use of the term approve or approval indicates that the responsible originating official, or designated decision authority, of a document, report, condition, waiver, deviation, etc. has agreed, via their signature, to the content and indicates the document is ready for release, baselining, distribution, etc.
- A.3 Assessment – An objective evaluation of performed processes or products and services against their applicable process descriptions, standards, procedures, and requirements.
- A.4 Audit – An examination of a work product or set of work products performed by a group independent from the developers to assess compliance with specifications, standards, contractual agreements, or other criteria. [Based on IEEE 610.12, IEEE Standard Glossary of Software Engineering Terminology]
- A.5 Concur - For this document, the use of concur or concurrence means to agree and accept, via signature, the readiness and content of a condition, requirement, report, deviation, document, etc. This also implies that if the stakeholder (e.g. SMA) does not concur, that their sign-off is withheld and the document, waiver, deviation package, test report, hazard report, etc. is not to be considered acceptable until such changes are made to achieve agreement on the deliverable.
- A.6 In-house Program/Project – A program/project that is implemented within the customer organization rather than by a system or integration contractor.
- A.7 Insight – Surveillance mode requiring the monitoring of customer-identified metrics and contracted milestones. Insight is a continuum that can range from low intensity, such as reviewing quarterly reports, to high intensity, such as performing surveys and review.
- A.8 Oversight – Surveillance mode that is in line with the supplier's processes. The customer retains and exercises the right to concur or nonconcur with the supplier's decisions. Nonconcurrence must be resolved before the supplier can proceed. Oversight is a continuum that can range from low intensity, such as customer concurrence in reviews (e.g., PDR, CDR), to high intensity oversight, in which the customer has day-to-day involvement in the supplier's decision-making process (e.g., hardware/software inspections).
- A.9 Provider – The entities or individuals that design, develop, implement, test, operate, and maintain the software products. A provider may be a contractor, a university, a separate organization

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

within NASA, or within the same organization as the acquirer. The term “provider” is equivalent to “supplier” in ISO/IEC 12207, Software life cycle processes.

- A.10 Reliability – The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions.
- A.11 Review – [1] A process or meeting during which a software product or related documentation is presented to project personnel, customers, managers, software assurance personnel, users or user representatives, or other interested parties for comment or approval. [IEEE 610.12, IEEE Standard Glossary of Software Engineering Terminology] Reviews include, but are not limited to, requirements review, design review, code review, test readiness review. Other types may include peer review and formal review.
- [2] An examination and analysis of documentation to evaluate the feasibility, capability, appropriateness, relevance, and effectiveness of documented processes and procedures for defining, imposing, implementing, and verifying SMA requirements. It is a necessary precursor to an audit or assessment. Review findings are provided to the organization being evaluated and to senior Agency management (e.g., Chief, Safety and Mission Assurance, Chief Engineer, Mission Director, Center Director, Center SMA Director).
- A.12 Software – Computer programs, procedures, scripts, rules, and associated documentation and data pertaining to the development and operation of a computer system. Software includes programs and data. This also includes COTS, GOTS, MOTS, reused software, auto generated code, embedded software, firmware, and open source software components.
- A.13 Software Safety – The discipline of software assurance that is a systematic approach to identifying, analyzing, tracking, mitigating, and controlling software hazards and hazardous functions (data and commands) to ensure safe operation within a system.

<b>DIRECTIVE NO.</b>	800-PG-7150.4.1
<b>EFFECTIVE DATE:</b>	July 15, 2013
<b>EXPIRATION DATE:</b>	July 15, 2020

Page 16 of 17

## Appendix B – Acronyms

COTS	Commercial Off-The-Shelf
GOTS	Government Off-The-Shelf
GPR	Goddard Procedural Requirements
GSFC	Goddard Space Flight Center
IEEE	Institute of Electrical and Electronics Engineers
MOTS	Modified Off-The-Shelf
NASA	National Aeronautics and Space Administration
NPR	NASA Procedural Requirement
PDL	Project Development Lead
PG	Procedures and Guidelines
RSM	Range Safety Manual
SIMS	Software Inventory Management System
SMA	Safety and Mission Assurance
STD	Standard
SQA	Software Quality Assurance
WFF	Wallops Flight Facility

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



**DIRECTIVE NO.** 800-PG-7150.4.1  
**EFFECTIVE DATE:** July 15, 2013  
**EXPIRATION DATE:** July 15, 2020

Page 17 of 17

## CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	July 15, 2013	Initial Release
	July 12, 2018	Administratively Extended with no changes for approximately one year while waiting for the NPR 7150.2 and the NASA Standards on Software Assurance and Software Safety are being revised.
	July 11, 2019	Administratively extending for 1 year

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.